Trick or Heat? Manipulating Critical Temperature-Based Control Systems Using Rectification Attacks

Yazhou Tu*
University of Louisiana at Lafayette
yazhou.tu1@louisiana.edu

Sara Rampazzi*
University of Michigan
srampazz@umich.edu

Bin Hao
University of Louisiana at Lafayette
bin.hao@louisiana.edu

Angel Rodriguez
University of Michigan
angelrod@umich.edu

Kevin Fu
University of Michigan
kevinfu@umich.edu

Xiali Hei
University of Louisiana at Lafayette
xiali.hei@louisiana.edu

ABSTRACT

Temperature sensing and control systems are widely used in the closed-loop control of critical processes such as maintaining the thermal stability of patients, or in alarm systems for detecting temperature-related hazards. However, the security of these systems has yet to be completely explored, leaving potential attack surfaces that can be exploited to take control over critical systems.

In this paper we investigate the reliability of temperature-based control systems from a security and safety perspective. We show how unexpected consequences and safety risks can be induced by physical-level attacks on analog temperature sensing components. For instance, we demonstrate that an adversary could remotely manipulate the temperature sensor measurements of an infant incubator to cause potential safety issues, without tampering with the victim system or triggering automatic temperature alarms. This attack exploits the unintended rectification effect that can be induced in operational and instrumentation amplifiers to control the sensor output, tricking the internal control loop of the victim system to heat up or cool down. Furthermore, we show how the exploit of this hardware-level vulnerability could affect different classes of analog sensors that share similar signal conditioning processes.

Our experimental results indicate that conventional defenses commonly deployed in these systems are not sufficient to mitigate the threat, so we propose a prototype design of a low-cost anomaly detector for critical applications to ensure the integrity of temperature sensor signals.

CCS CONCEPTS

• **Security and privacy → Embedded systems security**.

*Tu and Rampazzi are co-first authors.
Corresponding faculty authors: S. Rampazzi, K. Fu, X. Hei

CCS '19, November 11–15, 2019, London, United Kingdom

ACM ISBN 978-1-4503-6747-9/19/11…$15.00
https://doi.org/10.1145/3319535.3354195

KEYWORDS

Hardware Security; Safety-Critical Systems; Sensor Signal Injections; Temperature Sensors

ACM Reference Format:
Yazhou Tu, Sara Rampazzi, Bin Hao, Angel Rodriguez, Kevin Fu, and Xiali Hei. 2019. Trick or Heat? Manipulating Critical Temperature-Based Control Systems Using Rectification Attacks. In *2019 ACM SIGSAC Conference on Computer and Communications Security (CCS '19), November 11–15, 2019, London, United Kingdom.* ACM, New York, NY, USA, 15 pages. https://doi.org/10.1145/3319535.3354195

1 INTRODUCTION

Embedded systems that utilize temperature sensors are extensively employed in the supervision and automatic control of temperature-sensitive environments such as in hospitals, laboratories, and industrial and manufacturing facilities [18, 28, 39, 69]. In particular, closed-loop temperature control systems have become indispensable in many critical applications such as infant incubators that maintain the thermal stability of low birth weight or sick newborns [6], and blood bank or vaccine refrigerators that provide an optimal preservation temperature in the cold chain [7, 10].

In this paper, we present a research study on the reliability of temperature-based control systems and their sensors. Our study is driven by the importance of security in safety-critical temperature-based control systems and concerns about potential consequences caused by compromised sensors. It may not be safe to assume that these automatic systems would always behave as users expected or could always be carefully attended to by alert human operators. Moreover, some adverse effects caused by unsafe temperatures can be subtle and may not be detected immediately. We notice that there are reports about how safety issues can be related to improper temperature control [27, 62, 75, 82]. For instance, deaths and injuries to neonates in incubators have been linked to thermostat failure that caused incubator overheating and infant hyperthermia [6]. In one case of a fatal incubator malfunction, an infant incubator overheated and resulted in the death of a baby [75]. While the incubator's alarm went off, the nurses did not hear it because of the noisy, busy environment in the neonatal intensive care unit. Besides, poor refrigeration could make vaccines ineffective and leave the patients unprotected against dangerous diseases, or increase the risk of bacterial proliferation in blood products and cause potentially life-threatening transfusion reactions [12, 27, 82]. Therefore, it is necessary to investigate and understand the security and reliability of critical temperature-based control systems.

Our study focuses on physical-level attacks that exploit weaknesses in temperature sensors to manipulate temperature-based control systems. We show that, without tampering with the target system, adversaries can remotely manipulate the control system or circumvent temperature alarms by spoofing the temperature sensor with electromagnetic interference (EMI) signals. Unlike previous works that utilize the generation of subharmonics in non-linear circuit components to demodulate out-of-band EMI signals [56], or induce signal clippings in Electro-Static Discharge (ESD) protection circuits of a microcontroller [71], our attack exploits the unintended rectification effect in operational and instrumentation amplifiers to generate a controllable DC component on the amplifier output that can be used to manipulate the sensor readings (Fig. 1). We conduct detailed signal injection experiments on a typical temperature sensing circuitry and show that a stabilized voltage level can be intentionally induced and controlled to increase or decrease the sensor output. We analyze the vulnerability and attack surface of circuit components with both direct power injection (DPI) and remote signal injection experiments. We then investigate the effect of remote attacks on several off-the-shelf temperature sensors and control systems that use different amplifiers. In addition, we show how this physical-level exploit can affect other classes of sensors that share similar signal conditioning processes.

To explore potential consequences and understand the threats of physical-level attacks on critical temperature-based control systems, we study our attacks on an infant incubator and other real-world systems. In particular, we show how an adversary can remotely manipulate an infant incubator temperature to cause life-threatening issues. Without triggering the automatic temperature alarms, the attack can trick the internal control system of the infant incubator to heat the cabin up to $38.5°C$ or cool it down to $29°C$, from attack distances of 1.9 m and 1 m respectively in the open air with a transmitting power of 4 W. These dangerous temperatures can raise the risk of temperature-related health issues in infants, such as hyperthermia and hypothermia, which in turn can lead to hypoxia, neurological complications, and even death [8, 59, 78]. We also investigate the threats on several systems equipped with different types of temperature sensors such as laboratory thermal control equipment and 3D printers. Our experimental results show that these systems blindly trust the spoofed temperature sensor readings, resulting in manipulated decision makings of the victim system.

Our study illustrates the threat of exploiting a low-level vulnerability of temperature sensors in critical control systems and the necessity to mitigate this vulnerability. We discuss several conventional defenses, such as filtering and shielding, as well as their limitations. To enhance the robustness of critical temperature-based control systems and shed light on defenses against rectification attacks on sensors, we propose a low-cost anomaly detector that identifies malicious interference in the vulnerable frequency range. Once the interference is detected, the signal information can be used by the system software to estimate the sensor data reliability. Our study aims to raise the awareness of potential threats of compromising temperature sensors and work towards improved security and resilience in future designs of critical temperature-based systems.

In summary, we list our main contributions as follows:

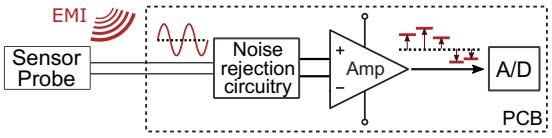

Figure 1: An illustration of the general signal conditioning path of a temperature sensor. Our attack can bypass conventional noise filtering and generate a controllable DC voltage offset at the ADC input.

- We investigate the reliability of temperature-based control systems and their sensors from a security and safety prospective. We explore how unexpected consequences can be caused in real-world systems with physical-level attacks on temperature sensors[1].
- We bridge the gap of sensor security research by explaining how to manipulate the DC voltage of temperature sensor signals, characterizing the rectification effect that can be intentionally induced in amplifiers. By analyzing the attack surface of circuit components with DPI and remote EMI injection experiments, we unveil the fundamental causality of the vulnerability. Furthermore, we show that the exploit of the rectification phenomenon could affect other classes of sensors that use similar vulnerable components.
- Based on the experimental results of our study, we discuss conventional defensive strategies, their limitations and challenges; then we propose a prototype design of an analog anomaly detector to enhance the security and reliability of temperature-based control systems.

2 BACKGROUND

In this work, we focus on the security of systems based on three types of analog temperature sensors: thermocouples, Resistance Temperature Devices (RTDs), and thermistors. Thermocouples operate on the Seebeck effect, which occurs when two dissimilar metals are joined at one end. The output voltage is a direct function of the temperature difference between the junction of the metals and the target measurement point [69]. RTDs are constructed of a metal, such as copper or platinum, which increases in resistance with increasing temperature. Compared to thermocouples, they require voltage or current excitation, and are generally more sensitive. Finally, thermistors are made of metal oxides and may have either a negative or positive temperature coefficient. Negative temperature coefficient thermistors (NTCs) decrease in resistance with increasing temperatures, while positive temperature coefficient thermistors (PTCs) increase in resistance with increasing temperatures. Thermistors exhibit a much greater sensitivity than thermocouples or RTDs. However, their operating temperature range is narrower.

Signal Conditioning of Analog Temperature Sensors. Analog sensors require a signal conditioning phase before a data acquisition device can effectively process the signal. Analog temperature sensors present specific signal conditioning requirements to provide reliable and accurate measurements. For instance, the relationship between the output voltage and the temperature measurements

[1]Demo videos of the proof-of-concept attacks are available at https://www.youtube.com/playlist?list=PLZaFM1g7JkPgpieNXMomMTQ7w9iZ8Yn-3.

is not linear, and each type of sensor exhibits its distinctive non-linearity. For this reason, analog temperature sensors often require high-resolution ADCs to achieve the desired accuracy [52]. Also, thermocouples require an additional correction to the acquired measurement called Cold-junction compensation (CJC). CJC accounts for the voltage offset generated at the connection between the thermocouple and the terminals of the acquisition device. In comparison, RTDs are often placed in bridge circuits for detecting small resistance changes. These additional considerations are used to improve the measurement accuracy.

Furthermore, because of the low-level voltage, the output signal from analog temperature sensors needs to be properly filtered and amplified before further processing can occur (Fig. 1). RTDs and thermistors voltage outputs are usually amplified by operational amplifiers (op-amps), while thermocouples use instrumentation amplifiers (in-amps) [54]. Both types of amplifiers provide the very important function of extracting the small signals from the temperature sensors, and also providing the adequate common-mode noise rejection[2]. Filters, on the other hand, block out both common and differential-mode noise, and the interference induced by the 50/60 Hz power.

Inadequate design specifications of these fundamental components can be exploited by an adversary to gain control over the sensor and induce the target system to make automated decisions based on untrustworthy sensor data.

Rectification Effect in Amplifiers. The rectification effect in amplifiers is a phenomenon that converts AC signals in input to an amplifier to a DC offset component in the output signal. This offset is the result of the non-linear voltage-current characteristics of the internal diodes formed by silicon p-n junctions inside the transistors (FETs or BJTs) that constitute the amplifier internal input stage [3, 40, 41, 84]. Generally, the operating point of an amplifier, also known as quiescent point, is the DC bias required by an amplifier to operate correctly and amplify the input signal without distortion. Especially in low-power amplifiers, where the input stage transistors works at low current and low impedance levels, a high frequency sine wave injection can alter the bias level of the amplifier, generating a DC offset in the output signal.

For example, considering a small AC voltage V_x at frequency ω_x injected across the base-emitter junction $\Delta V = V_x cos(\omega_x t)$ of an operational amplifier BJT-based input stage, the collector current around the quiescent point can be express as $I'_C = I_C(V_{BE} + \Delta V)$ where V_{BE} is the base-emitter voltage. Applying the Taylor series expansion of the transistor collector current we can observe three main spectral components: the quiescent collector current I_C, $cos(\omega_x t)$ and $cos^2(\omega_x t)$. While the linear spectral term is filtered by other stages within the device, the quadratic term remains and contains two components, one depended by twice of the signal input frequency ($2\omega_x$) and a DC term [3]. This DC term is the rectification effect, that can be expressed as a variation of the quiescent collector current:

$$\Delta i_C = (\frac{V_x}{V_T})^2 \cdot \frac{I_C}{4} \quad (1)$$

where V_T is a constant equal to 25.68 mV at 25 $^\circ C$ for BJT based amplifiers [3]. In FET-input operational amplifiers the rectification term of the drain current I_D become $\Delta i_D = (\frac{V_x}{V_P})^2 \cdot \frac{I_{DSS}}{2}$ where I_{DSS} is the drain current at zero gate-source voltage, and V_P the pinch-off voltage.

The analysis shows how the rectification effect in op-amps is directly proportional to the square of the injected AC signal's amplitude, independently by the type of transistor used [3].

In addition, instrumentation amplifiers are generally composed by three op-amps, where the first two are arranged to buffer each input to the third one. Wu et al. [84] demonstrated that the rectification effect mainly happens at the non-inverting input of two op-amps in the first stage of an in-amp. Furthermore, the resulting DC offset at the in-amp output increases if the DC voltage difference between the inverting input and the non-inverting input of the third op-amp becomes higher. Therefore, to reduce the rectification effect, external noise signals should be eliminated before the amplifier input with proper filtering.

Our remote attack targets temperature-based control systems lacking effective noise suppression circuits, tuning the transmitted EMI signals to a carrier frequency equal to the resonant frequency of the target circuit component to maximize the injected AC voltage and induce the rectification effect.

3 THREAT MODEL

The goal of the adversary is to spoof the temperature sensor measurement and manipulate a temperature control system to heat up or cool down to an unsafe temperature. The adversary cannot tamper with any hardware or software of the target system. Also, we don't consider a malicious human operator that could directly affect the actual temperature around the sensor or deliberately operate the victim system to manipulate the temperature setpoints of the system.

Attack Scenarios. Adversaries could launch the attack from one to several meters away, depending on their equipment and susceptibility of the victim system. Furthermore, the malicious EMI signals can penetrate many common physical barriers such as walls and windows. For instance, the attack could be launched from outside of a wall/window or from adjacent rooms. An adversary could also use a hand-held attack device that can be carried and surreptitiously operated under his/her clothes. Additionally, the adversary might secretly leave or install a small remote control EMI emitting device around the victim system in advance of the attack. During the attack, two parameters (frequency and amplitude of EMI signal) need to be adjusted.

Equipment. Adversaries could use commodity signal generators, amplifiers and antennas to emit malicious EMI signals. Alternatively, adversaries could purchase or make a customized small portable transmitter to conduct the attack; the device would be similar to a hand-held radio transmitter (e.g., walkie-talkie) but with gain control and a frequency range that covers the attack frequencies. The power of EMI emitters that we use in experiments is below 4 W, but more capable adversaries might use more specialized equipment and techniques to improve the attack.

[2]Depending on the conduction mode, differential-mode (or normal-mode) noise appear across the lines of an electric circuit following the same direction as the power supply current. In contrast, in common-mode noise, current flows in the same direction along different lines with the same voltage with reference to the earth [43].

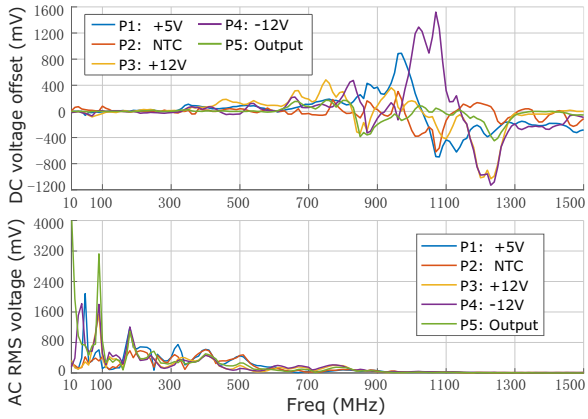

Figure 2: The results of DPI experiments on different injection points of the experimental circuitry. We record the induced DC voltage offset and the RMS voltage of AC signals corresponding to different EMI frequencies.

Feedback. We assume that the adversary can observe the temperature readings or heating/cooling indicator lights in the target system, to ensure the induced attack effect. Alternatively, another adversary or a monitoring device could help observe the feedback of the victim system. However, the adversary does not have to observe the victim system all the time; after the adversary ensures the attack effect and selects suitable frequencies and amplitudes of attack signals, observations will no longer be needed.

4 COMPROMISING TEMPERATURE SENSORS

In this section, we conduct detailed signal injection experiments on typical temperature sensing circuits to study the attack effect. We analyze the vulnerable circuit components and attack surface with both DPI and remote EMI injection experiments.

4.1 Security Analysis

To explain how temperature sensors could be affected by rectification attacks, we build an experimental temperature sensing circuitry based on an NTC thermistor. We wire the thermistor in a bridge circuit. Bridge circuits are commonly used in the wiring of resistive sensors such as thermistors, RTDs and strain gauges [51]. The differential voltage generated by the bridge circuit is collected and amplified by a Texas Instruments (TI) LM1458 operational amplifier. The details of the setup can be found in the Appendix (Fig. 16).

Direct Power Injection (DPI) Experiments. It is difficult to measure and analyze the exact attack effect in circuits caused by remote EMI radiations since the path and strength of the induced EMI signals cannot be accurately predicted. Thus, we conduct DPI experiments to identify and analyze how EMI can affect internal components of temperature sensors.

In DPI, EMI signals can be injected directly into desired injection points on the circuit through conductance. In this way, we can control the power of the injected EMI signals more accurately and avoid interference from unintentional EMI radiations on other parts of the circuits. In our experiments, we connect the direct power injection circuit to each of the possible signal injection points on the sensing circuitry.

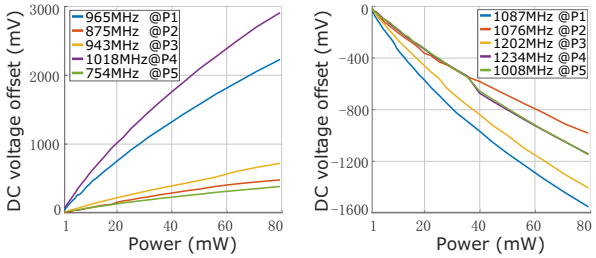

Figure 3: The relationship between the magnitude of the induced DC voltage offset and the power of directly injected EMI signals.

Inducing a Stabilized DC Voltage with Specific EMI Signals. To achieve adversarial control over the sensor output instead of general disruptions of the sensing system, we need to induce stabilized DC voltage levels to control the sensor output rather than fluctuating interference signals to disturb it. First, we find specific EMI signals that can be rectified by the amplification circuits to induce controllable voltage levels without causing strong noises. We inject single-tone sine-wave EMI signals to each injection point of the experimental circuitry and sweep the frequency from 10 MHz to 1.5 GHz at an interval of 10 MHz with an injection power of 15 dBm, which is equivalent to 32 mW. As shown in Fig. 2, we record the induced DC voltage offset as well as the root mean square (RMS) voltage of fluctuating alternating current (AC) signals in the output of the amplifier. We observe that EMI signals at specific frequencies induce a significant DC offset and the corresponding AC interference signal is below the typical noise floor. Such frequencies can be used in attacks to induce intentionally fabricated signals that cannot be easily distinguished from legitimate sensor measurements. Depending on the frequency of EMI signals, the induced DC offset in the experimental circuitry could be either positive or negative, allowing adversaries to increase or decrease the temperature measurement maliciously.

Attack Surface. The identification of the attack surface helps to understand possible attack mechanisms and facilitates the evaluation of sensor security in future system designs. As shown in Fig. 2, our DPI experiments validate that a stabilized DC voltage signal can be induced by EMI signals injected through different entry points, including the sensor wire as well as other parts of the circuitry such as shared power lines. As a result, adversaries could exploit sensor wires, relatively long cables or printed circuit board (PCB) traces to inject malicious EMI signals and induce the attack effect. The potential attack surface also includes other components in the system that are connected to the injection points of the sensing circuitry. For instance, EMI signals conducted through the charging port could affect a physically co-localized microphone in a smartphone [50]. Similarly, devices, cables and other components that are connected to possible injection points of the temperature sensing circuitry could also make the sensor more susceptible to attacks and need to be considered in the design of a system.

DC Voltage and EMI Power Relationship. Adversaries need to control the magnitude of the induced DC voltage to gain effective control over the sensor output. Theoretically, the magnitude of the induced DC voltage offset is directly proportional to the power of

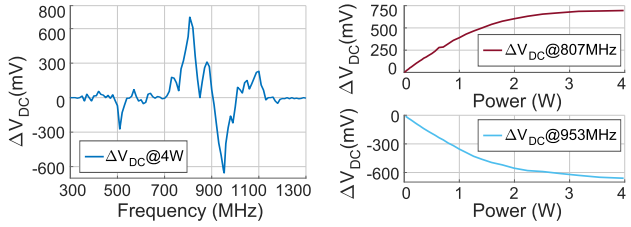

Figure 4: The relationship between the induced DC voltage offset and the attack frequency (left), and the relationship between the magnitude of the DC voltage offset and the transmitting power (right) in remote attacks.

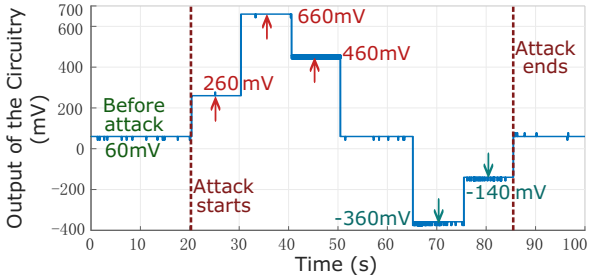

Figure 5: Remotely injecting stabilized voltage levels to control the output of the temperature sensing circuitry.

injected EMI signals as described in Eq. (1). Therefore, in the case of bipolar junction transistor (BJT) based amplifiers, the rectified DC current change ΔI can be described as $\Delta I = (\frac{V_{emi}}{V_T})^2 \cdot \frac{I_C}{4}$, where V_{emi} is the amplitude of injected EMI signals, I_C is the quiescent collector current of the transistor, and V_T is a constant. Assuming that the equivalent resistance of the receiving circuitry is R_r, the power of the injected EMI is P_r, we have $V_{emi} = \sqrt{P_r R_r}$. Therefore, we can represent the induced DC offset as

$$\Delta V_{DC} = \Delta I R_r = (\frac{V_{emi}}{V_T})^2 \cdot \frac{I_C}{4} R_r = (\frac{R_r}{V_T})^2 \cdot \frac{I_C}{4} P_r \quad (2)$$

We conduct DPI experiments on the experimental circuitry and inject EMI signals to each of the injection points to validate the effectiveness of the theoretical analysis. We select the EMI frequencies that correspond to peaks and troughs in Fig. 2 to affect the output of the amplifier. As shown in Fig. 3, the power of directly injected EMI signals is positively related to the magnitude of the induced DC offset. The relationship can be considered as locally proportional but presents a changing rate that gradually decreases as the power of injected EMI signals grows.

For simplicity, we utilize the free space propagation model to understand the relationship between the transmitting power (P_t) and the injected power (P_r) in remote attacks. From the Friis transmission equation, we have

$$P_r = G_t G_r (\frac{\lambda}{4\pi D})^2 P_t \quad (3)$$

G_t and G_r are the gains of the transmitting and receiving antennas respectively. G_t depends on the type of antenna that is used by the attacker. Note that components in the victim circuit work as a receiving antenna. λ is the wavelength of EMI signals. D is the attack distance between the adversary's antenna and the victim circuit. Based on Equations 2, 3, and our previous analysis, we can

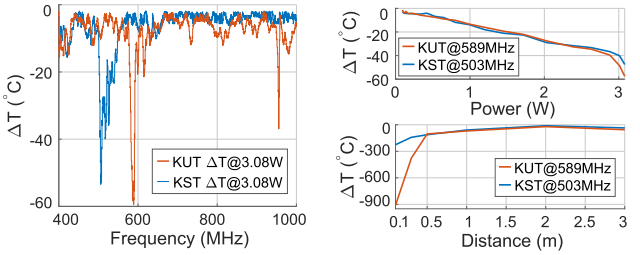

Figure 6: Results of remote attack experiments on K-type shielded (KST) and unshielded (KUT) thermocouples connected to the MAX31855K amplifier with an attack distance of 3 m in the open air (left and right top). The induced temperature change in different attack distances with a transmitting power of 3.08 W (right bottom).

infer that the magnitude of the induced DC voltage signal is locally proportional to the power of transmitting EMI, which will be validated in our remote EMI injection experiments.

Spoofing the Temperature Sensor Output. We investigate remote EMI injections that leverage the rectification effect in amplifiers to gain adversarial control over the output of the temperature sensing circuitry. As shown in Fig. 4, we transmit single-tone sinewave EMI signals and sweep the frequency from 300MHz to 1 GHz at an interval of 10 MHz with a transmitting power of 36 dBm (equivalent to 4 W) and observe the induced DC voltage offset on the oscilloscope. We find that the maximum and minimum DC voltage offsets are induced at around 810 and 950 MHz respectively. We then adjust the frequency of EMI signals with an interval of 1 MHz to find the most effective frequencies that can be used in remote attacks to maliciously increase or decrease the output voltage of the circuitry. During the experiments, we shield the PCB with a metal box and cover the probe of the oscilloscope with aluminum shielding sleeves to mitigate unintentional interference. We aim EMI signals to the sensor wire with a directional antenna [19] from a horizontal distance of 0.2 m.

We demonstrate how adversaries can intentionally induce stabilized voltage levels to control the output of the temperature sensing circuitry by remote rectification attacks (Fig. 5). In the experiment, we increase the output of the circuitry by using an attack frequency of 807 MHz and decrease it with a frequency of 953 MHz. We manipulate the magnitude of the injected DC voltage level by adjusting the transmitting power between 0 and 2 W at an attack distance of 0.2 m. We monitor the real-time analog output of the circuitry with the oscilloscope and record it with an Arduino UNO R3 microcontroller that is connected to a laptop.

4.2 Off-The-Shelf Temperature Sensors

We investigate the attack effect on several off-the-shelf temperature sensor circuits that use different amplifier breakout boards.

Thermocouple Sensors. We investigate the attack effects on both shielded and unshielded K-type thermocouples that are connected to a Sparkfun MAX31855K amplifier breakout board [9] with a digital output interface, and an Adafruit AD8495 amplifier breakout board [11] that has an analog output interface.

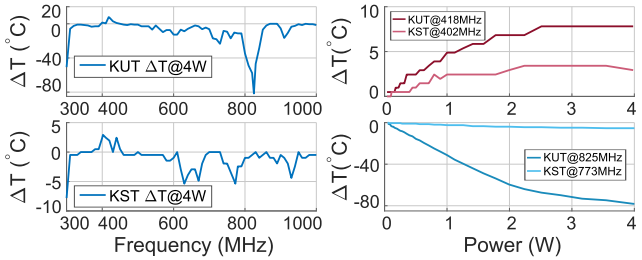

Figure 7: Results of remote attack experiments on thermocouples connected to the AD8495 amplifier with an attack distance of 0.6 m.

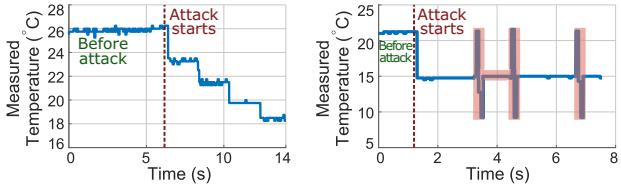

Figure 8: Remote control of a K-type shielded thermocouple at 1 m distance in two different scenarios: generating a step function (left) and spelling of the word "HI" (right).

The length of the thermocouples we test is 1 m and we use an Arduino board to sample the output of the Sparkfun MAX31855K breakout board. As shown in Fig. 6, with an attack frequency of 589 MHz and an emitting power of 3.08 W, the attack can decrease the temperature measurement of the unshielded thermocouple by about $56°C$ or $909°C$ from an attack distance of 3 m or 0.1 m respectively. We also conduct the remote attack experiments on the Adafruit AD8495 breakout board using a similar setting and summarize the results in Fig. 7.

Spoofing Attacks on Thermocouples. Adversaries that have capabilities to deliver EMI to a victim thermocouple sensor circuitry can remotely spoof the sensor output and inject arbitrary, attacker-chosen temperature values. We remotely inject spoofed temperature measurements to a K-type shielded thermocouple that is connected to the MAX31855K amplifier with an attack distance of 1 m and a transmitting power below 3.08 W. Our experiments demonstrate the control over the temperature sensor output in two different scenarios (Fig. 8). We use amplitude-modulated EMI signals to control the sensor measurements. We assume a sinusoidal carrier signal $c(t) = A(t) \cdot \sin(2\pi f t)$, where A is the amplitude of the signal, t is the time, and f represents a frequency that induces a DC voltage offset in the output of the victim circuitry. We vary the amplitude A over time, according to the different scenarios.

Experiments with RTDs. We test both shielded and unshielded PT100 RTDs connected to an Adafruit MAX31865 amplifier breakout board [23] with remote EMI injection experiments. First, we generate EMI signals with antennas and sweep the frequency from 10 MHz to 1.5 GHz but could not observe a stable temperature change induced in the output of sensor. We then inject conducted EMI signals directly into the terminals of the MAX31865 board connected to the RTD and sweep through a wider frequency range. As shown in Fig. 9, we find that EMI signals with lower frequencies around 1 or 2 MHz can be more effective to manipulate the temperature measurement.

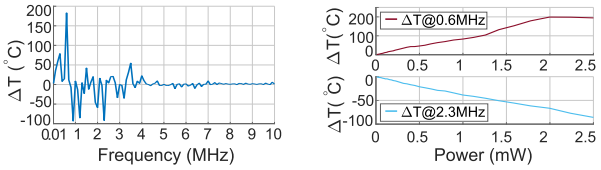

Figure 9: DPI experiments on the RTD circuitry with an injection power of 2.5 mW (left). The amount of induced temperature change with different injection power (right).

5 MANIPULATING TEMPERATURE-BASED CONTROL SYSTEMS

In this section, we investigate the threats of the attack on real-world temperature-based control systems that use different kinds of temperature sensors, including NTC/PTC thermistors, thermocouples and RTDs. We evaluate the attacks on systems that are employed in medical applications such as an infant incubator, and in laboratory equipment that control critical biological experiments or manufacturing processes. Additionally, we investigate several commodity PID controllers equipped with temperature alarm functions.

We summarize the results of our attack experiments in Table 1. We show that embedded systems based on different kinds of temperature sensors employed in different application areas can be affected by our attacks. Our results validate that temperature-based control systems blindly trust temperature sensor readings to make automated decisions, which allows adversaries to exploit and abuse them for causing unintended consequences.

Many of the systems we test have external temperature sensor probes that need to be deployed to measure the temperature of a specific environment. Usually, the wiring and interfaces of systems with external sensors could make the system more susceptible to our attacks. Devices with internal temperature sensors might be less susceptible but can still be affected. For instance, the UVP HB-500 hybridization oven is covered by metal panels and most part of the internal sensor wire is protected by additional aluminum foil, but we notice that small gaps between the metal panels could allow EMI signals to pass through and be picked up by internal cables or PCB traces. In addition, control panels of many devices can allow EMI signals to enter the system. The control panels consist of various user interface components such as screens, buttons and lights; EMI signals could pass through the spaces between these components. Moreover, the cables connected to components in the control panel or peripheral devices could also pick up EMI signals and might conduct the signals into possible injection points of the victim temperature sensing circuitry.

Experimental Settings. The maximum transmitting power of our equipment is 36 dBm, which is equivalent to 4 W. We use a ZHL-4240 amplifier that has an average gain of about 44 dB in the range of 10 MHz to 2 GHz [17]. The signal source is an Agilent N5172B vector signal generator. We use a directional antenna [19] that has a length of 0.5 m to emit sinusoidal EMI signals with frequencies above 300 MHz, and an extendable dipole antenna for frequencies below 300 MHz. For most of the devices, we sweep through 300 MHz to 1 GHz with an interval of 10 MHz and observe the temperature measurement of the device to find the attack frequencies. We then adjust the frequency with a step of 1 MHz to find the optimal

Table 1: Results of attack experiments on real-world temperature-based control systems

Device	Sensor† Type	Applications	$\Delta T_{Max@0.1m}(^{\circ}C)$ /Freq. (MHz)	$\Delta T_{Min@0.1m}(^{\circ}C)$ /Freq. (MHz)	Max. Attack Distance‡(m)
Air-Shields Isolette C100 Incubator	NTC	Medical Device	+58.4/530	-15.9/847	5.8 *
Fisherbrand Traceable Thermometer	NTC	Biomedical, Lab	+37/690	-22/730	3.4 *
Thomas Traceable Thermometer	NTC	Biomedical, Lab	+16/640	-50/830	1.6
UVP HB-500 Hybridization Oven	PTC	Laboratory	+42.4/516	-2.8/453	3.3
Revolutionary Science Incufridge	Un	Laboratory	+0.9/308	-3.3/309	0.6
Sun Electronic EC12 Thermal Chamber	KTC	Manufacturing, Lab	+3.35/686	-2.88/1300	0.3
MakerBot 3D printer Smart Extruder +	KST	Manufacturing, Lab	+10/1000	N/A	0.25
Inkbird ITC-100VH Controller	KST	IoT	>+78/556	N/A	11.5 *
Inkbird ITC-1000F Controller	NTC	IoT	N/A	-10.6/713	0.9
Inkbird ITC-100RH Controller	RTD	IoT	>+80.9/453	N/A	16.2 *

† NTC/PTC: NTC/PTC thermistor, KTC: K-type thermocouple, KST: K-type shielded thermocouple, Un: Unknown.
‡ The maximum distance that we could induce a change of $0.5^{\circ}C$ in the temperature measurement with a transmitting power of 4 W. ∗ Estimated.

attack frequency. If we could not find the attack frequencies for a device in this range, we would sweep through the frequency ranges of 10 to 300 MHz and 1 to 2 GHz. In Table 1, we record the maximum increase or decrease that can be induced in the temperature measurement of the target system and corresponding EMI frequencies with an attack distance of 0.1 m. For the Inkbird ITC-100VH and ITC-100RH controllers, the manipulated temperature can exceed the maximum temperature range of the device at an attack distance of 0.1 m. We also record the maximum horizontal distance between the antenna and the target device that a change of $0.5\ ^{\circ}C$ can be induced in the temperature measurement. For several devices, the maximum attack distance is out of the dimension of our room setup, so we estimate the maximum distance based on our indoor measurements and the relationship between the induced temperature change and the attack distance (From Equations 2 and 3, we have $\Delta V_{DC} \propto \frac{1}{D^2}$).

5.1 Medical Applications

5.1.1 Infant Incubator. Newborn infants regulate body temperature much less efficiently than adults [1]. Infant incubators are critical medical devices widely used in neonatal care units. These incubators help maintain the thermal stability of infants - especially preterm or sick newborns [6, 28, 65]. The temperature inside the cabin of incubators is measured and adjusted, via a closed-loop temperature control system, to reside within an ideal preset temperature range, minimizing the risks of morbidity and mortality [8, 59, 78].

To maintain the infant in a Neutral Thermal Environment (NTE [25]), the closed-loop temperature control system in incubators can operate in skin servocontrol mode (skin-mode) or air temperature control mode (air-mode). The skin-mode is designed to maintain the neonate's abdominal skin temperature constant, whereas the air-mode is based on the control of the circulating incubator air temperature [34]. The simplest way to achieve a thermoneutral environment is to maintain a constant abdominal skin temperature between $36.0^{\circ}C$ and $36.5^{\circ}C$, in the skin-mode. This range minimizes the number of calories needed to maintain normal body temperature and reduces the risks of cold stress or overheating [30]. Usually, NTC thermistors are used in infant incubators to measure the skin

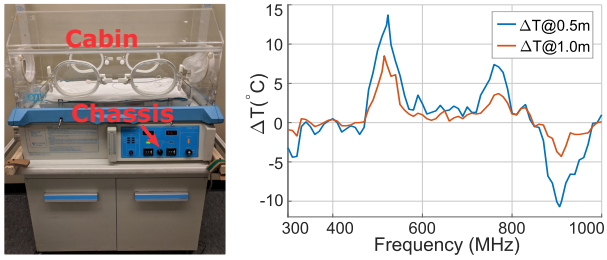

Figure 10: Infant incubator (left). The relationship between the induced change in the skin temperature measurement of the incubator and the attack frequency with a transmitting power of 4 W (right).

or air temperature and provide real-time feedback to the closed-loop temperature control system.

To find out whether the temperature control system of an infant incubator can be maliciously controlled and abused by adversaries to cause safety issues, we investigate our attacks on an Air-Shields Isolette C100 infant incubator [13]. We observe that the chassis of the incubator is shielded with aluminum panels. However, the large control panel, sensor interfaces, and air circulation holes on the chassis could still allow EMI signals to enter and affect the internal system components. In our experiments, we aim the antenna to the front control panel of the infant incubator. However, attacks from other directions are also possible (e.g., targeting the back of the chassis from an adjacent room).

Using a transmitting power of 4 W, our attack can maliciously control the skin temperature sensor measurement of the infant incubator with certain attack distances. As shown in Fig. 10, an adversary can increase the skin temperature measurement by $8.5^{\circ}C$ or decrease it by $4.3^{\circ}C$ from 1 m away with attack frequencies of 515 MHz and 910 MHz respectively. Additionally, the air temperature sensor measurement of the incubator could also be affected by the attack, but the amount of the induced change is less significant (about $1.5^{\circ}C$ at an attack distance of 0.2 m). To understand possible attack distances that can cause safety threats in the incubator with a certain transmitting power, we measure the maximum increase and decrease that can be achieved with different attack distances using a transmitting power of 4 W (Fig. 11). We observe that when we change the distance, the optimal attack frequency deviates slightly

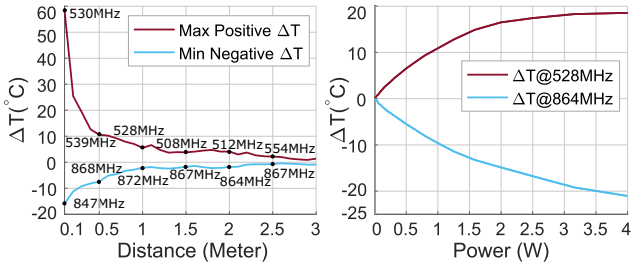

Figure 11: Maximum increase/decrease in the skin temperature measurement that can be achieved with different attack distances using a transmitting power of 4 W (left). The relationship between the amount of induced changes in the measured skin temperature and transmitting power with an attack distance of 0.2 m (right).

within a range of several tens of MHz. This could be caused by environmental changes when we change the distance. For instance, transmitting paths of reflected signals in the experimental area might have changed; and conductivity of objects nearby might affect the radiation pattern and impedance of the antenna. We also measure the relationship between the amount of induced changes in the measured skin temperature and transmitting power (Fig. 11). The relationship is consistent with the results of our experiments on temperature sensor circuitry in Section 4.

Temperature Alarms. During the experiments, the incubator is functioning in the skin-mode. We notice that when the manipulated skin temperature measurement significantly deviates from the preset skin temperature, an alarm would be triggered. The incubator system continuously compares the skin temperature measurement with the preset temperature value and raise the preset temperature alarm when a difference larger than $1°C$ is detected [13].

Additionally, a high temperature alarm would be triggered if the air temperature is over $38.5°C$. The alarm system of the incubator continuously monitors the measurement of an extra internal high air temperature sensor and raises the high temperature alarm when the temperature exceeds the maximum temperature limit. The high temperature limit is $38.5°C$ in the Air-Shields C100 incubator [13], and could be higher in other systems [2]. Finally, there is also a probe alarm function that detects shorted, open or disconnected conditions in air, skin, or high temperature sensors. However, the temperature alarm systems in incubators may not perform safety precautions reliably if the security of the system is compromised with physical-level attacks on temperature sensors. As a result, adversaries can manipulate the infant incubator system to cause safety issues without triggering any of these alarms.

Heating Attacks. An adversary can decrease the skin temperature measurement maliciously and trick the internal control loop of the incubator to actuate the heating system. With an attack distance of 2 m, an adversary that uses a transmitting power of 4 W can decrease the measured skin temperature by $1.8°C$ (Fig. 11). Adversaries can also launch the attack from an adjacent room. In our experiments, the infant incubator is placed 0.1 m away from a wall that has a thickness of 0.15 m and we target the back of the chassis from an adjacent room. With the wall between the adversary and the incubator, attacks with the same transmitting power can decrease the skin temperature measurement by $4.5°C$. As a result, the system would try to compensate for the induced temperature change to maintain the "preset temperature" by actuating the heaters.

To avoid being detected by the preset temperature alarm, adversaries can increase the transmitting power slowly and maintain the difference between the measured and preset temperature less than $1°C$. Adversaries can manipulate the system to reach and keep the maximum temperature of $38.5°C$ without triggering the high temperature alarm. This excessive temperature can result in hyperthermia in newborns with consequent dehydration, lethargy, seizures, apnea, increased risks of neurologic injury, etc. [8, 49].

Cooling Attacks. There is no automatic alarm to be triggered in the incubator if the cabin temperature drops below a specific minimum threshold. As a result, with an attack distance of 1 m, an adversary that uses a transmitting power of 4 W can manipulate the incubator to decrease the actual temperature from the preset $36°C$ to $29°C$, which is close to the room temperature during our experiment. Adversaries trick the infant incubator to actuate the cooling system by increasing the skin temperature measurement maliciously. For instance, with an attack distance of 2 m, an adversary can increase the skin temperature measurement by $4.2°C$ (Fig. 11). Using the same setup as the heating attack, an adversary in the adjacent room can increase the skin temperature measurement by $3.4°C$.

Moderate hypothermia occurs when the auxiliary temperature of an infant drops below $34.9°C$ and severe hypothermia can be caused when it drops below $32°C$ [8]. As we demonstrate, the attack can manipulate the infant incubator to decrease the actual temperature to the room temperature such as $29°C$ without triggering any alarm in the incubator system. The compromised incubator system would put the newborn at risks of serious and potentially life-threatening complications such as hypoxia, acidosis, cardiorespiratory and neurological complications, etc. [8, 59].

In our experiments, the time necessary to manipulate the incubator to raise the actual air temperature of the cabin to $38.5°C$ is less than 10 minutes; and it takes about 30 minutes to drop the actual temperature to below $32°C$. Nurses usually check and record the axillary temperature of newborns at a specific interval. Four hourly is the general recommended interval [25, 44]. When instability occurs, the interval can be every 30 to 60 minutes [25, 44]. Adversaries could exploit these intervals to pursue the attack.

5.1.2 Traceable Thermometers with Alarms. Traceable thermometers that provide highly-accurate temperature measurements are often used to monitor the quality of temperature-sensitive medication such as vaccines, or biological substances [24, 45]. They provide reliable temperature data records to assess the quality of substances being monitored and can raise an alarm when the storage temperature is out of a predefined range. We investigate our attacks on a Thomas traceable thermometer and a Fisherbrand traceable thermometer. Our experiments show that the integrity of the temperature data recorded by these thermometers can be compromised by attacks. For instance, with an attack distance of 0.5 m and a transmitting power of 4 W, an adversary can increase the temperature measurement of the Fisherbrand thermometer from $26°C$ to $49°C$ or decrease it to $20°C$. Malicious manipulations of the measurements can result in a recorded temperature data profile inconsistent with the actual quality of the biologic substances being

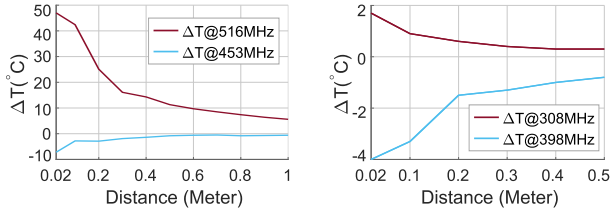

Figure 12: Maximum increase/decrease in the temperature measurement that can be achieved in attack experiments on the hybridization oven (left) and the incufridge (right) with different attack distances.

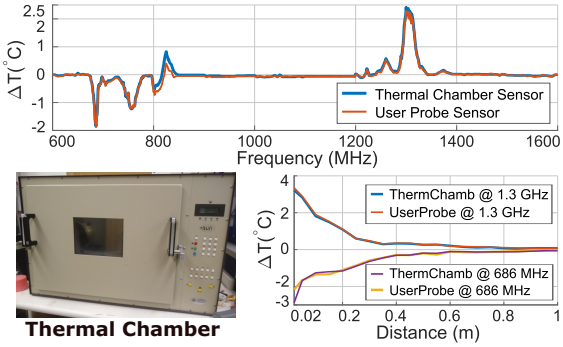

Figure 13: Temperature offsets induced on the thermal chamber with different attack distances using a transmitting power of 3.2 W. Note that the injection affect both the sensors in similar way despite the chamber shield.

monitored, which could lead to the waste of effective substances or the misuse of ineffective ones that should be discarded. Also, it is possible for adversaries to manipulate the measured temperature to suppress the alarm while the actual temperature is out of the safety range.

5.2 Laboratory Applications

5.2.1 Biological Laboratory Equipment. Temperature-based systems are widely used in biological laboratory equipment to preserve biological samples or control the temperature during critical experiments. These equipment are usually well-designed and are expected to control the temperature accurately because an unstable temperature environment can devastate valuable biological samples or bias the outcomes of experiments. However, in our experiments, we demonstrate how they can be maliciously compromised by adversaries.

We investigate our attacks on a hybridization oven and an incufridge. The UVP HB-500 hybridization oven accurately controls the temperature of samples in the hybridization process, enabling consistent saturation of sample solutions. It has an internal temperature sensor and is shielded with metal panels, but the gaps between these panels could allow EMI signals to pass through and affect internal circuit components. With an attack distance of 1 m, an adversary can maliciously increase the temperature measurement by 5.6$^{\circ}C$ and trick the hybridization oven to cool down.

The Revolutionary Science RS-IF-202 incufridge can be used to refrigerate or incubate specimens and biological products [4]. The incufridge has an internal temperature sensor and is well-shielded with metal panels. However, we find that EMI signals could enter through the control panel of the device, which can be exploited to spoof its temperature sensor measurement. In the experiments, we use a transmitting power of 4 W, and we summarize the experimental results in Fig. 12.

5.2.2 Thermal Chambers. Thermal chambers can provide an accurately controlled thermal environment for automatic environmental tests of critical components such as aircraft electronics, satellite antennas, and implantable stents [26]. Adversarial control or disruptions of these systems could damage expensive components or make the results of environmental tests unreliable.

We investigate our attacks on a Sun Electronic Systems EC12 thermal chamber that is intended for automated test systems and laboratory applications [5]. This well-shielded metal chamber is equipped with two K-type thermocouples: The first one (thermal chamber sensor) is hidden behind the control panel and it measures the internal temperature of the chamber; The second one (the user probe) can be used to directly monitor the temperature of the device under test. We set and maintain the temperature of the chamber at 30°C, then we turn off the heater circuit breaker to ensure that only the temperature offset caused by the attack is measured. In our experiments, we point the antenna towards the double-paned glass window of the chamber and sweep a frequency range of 550 MHz to 1.6 GHz using a transmitting power of 35 dBm, which is equivalent to 3.2 W. We monitor the temperature variations in both the thermal chamber probe and the user probe. Although the sensors are placed in different locations of the chamber and the thermal chamber sensor is protected by a metal internal panel, our attack induces similar effects on both of the sensors simultaneously (Fig. 13). We also measure the maximum increases or decreases that can be induced in the temperature measurements with different attack distances.

5.2.3 3D Printers. In 3D printers, extruders are crucial components that are responsible for heating and expelling the building material (filament). The temperature control system of an extruder constantly monitors and adjusts the temperature of its heating chamber. During the building process, the temperature of the heating chamber must be kept within a certain tolerance range to ensure the quality of the build and prevent buildups of the filament [38]. Compromising the temperature sensor reliability in this fundamental phase could disrupt the printing process or damage the product quality. We investigate our attacks on two different extruder models: the MakerBot Smart Extruder and the MakerBot Smart Extruder + (Plus). We install these extruders onto two identical MakerBot Replicators 3D printers. Both of the two models use K-type shielded thermocouple sensors. Note that we do not turn on the extruder heating/cooling cycle to prevent damage to the heating chamber. We wait until the temperature of the extruder naturally reaches the equilibrium at room temperature (23°C) before starting the attack.

We test the frequency range of 400 MHz to 1 GHz, observing the temperature change of the extruder on the 3D printer's display. During the test, we observe two main effects: 1) With an attack frequency of 400 MHz, the user panels of both of extruder models show that the extruder temperature is zero. Even after reloading the extruder monitoring system, the displayed temperature remains

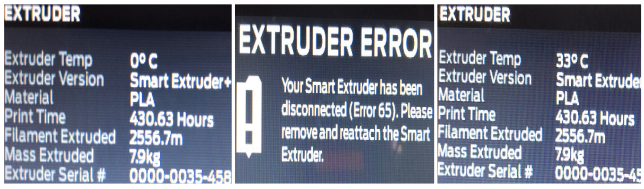

Figure 14: Results of our attack experiments on 3D printers. With a frequency of 400 MHz, the attack causes the disconnection of the extruder (left, middle). With an attack frequency of 1 GHz, the temperature perceived is $10°C$ higher than the actual temperature of $23°C$ (right).

zero (Fig. 14 left). When we start the "preheat" functionality, the device displays an extruder disconnection error message (Fig. 14 middle). 2) With an attack frequency of 1 GHz, we can increase the temperature measurement of the Smart Extruder Plus by a maximum of 10 °C compared to the baseline temperature (Fig. 14 right). In this case, the system does not give any error messages or special indications in the user panel when the measured extruder temperature is changed. Therefore, adversaries can spoof the temperature measurement to manipulate the temperature control system in the extruder without being detected by the system. In the experiments, we use a transmitting power of 3.2 W and we are able to induce a temperature change of $0.5°C$ at a maximum attack distance of 25 cm.

5.3 Consumer PID Controllers

We study the effect of our attacks on three consumer PID control modules: the Inkbird ITC-100VH, ITC-1000F, ITC-100RH. Although the modules we test are mainly used in IoT applications, devices with similar functions can be found in critical industrial and manufacturing applications [20–22]. The three modules are equipped with different types of temperature sensors. These devices can be used to limit or maintain the temperature of a target environment in a specific range. When the device detects a temperature that is out of the predefined range, it can raise the alarm to alert users or switch on/off the circuit of a heating or cooling element. Manipulation of temperature measurements can undermine the alarm function even when the actual temperature is out of the predefined range. Our experiments show that these modules are not well-shielded and can be susceptible to adversarial control with a relatively long attack distance. For instance, from a distance of 2 m, the attack can maliciously increase the temperature measurement of the ITC-100RH controller by a maximum of $32.9°C$ with an attack frequency of 453 MHz and a transmitting power of 4 W.

6 COUNTERMEASURES

Usually manufacturers implement filters to reduce external and internal electromagnetic interference, such as common-mode or differential-mode filters on the amplifier input [67]. However, as we demonstrate in our work, out-of-band EMI can induce AC signals that bypass generic filtering and be internally rectified through the amplifier input, output, or power supply pins. Although EMI defenses are known and some are already applied to certain critical applications [83], consumer electronics are less protected against malicious attacks that affect temperature sensors. In this section, we discuss and simulate several passive and active methods to detect or prevent EMI effects on temperature sensors.

6.1 Hardware Defenses

Traditional hardware defenses can take various forms according to the level of mitigation adopted and cost/performance limitations.

Shielding. Designing short shielded wires between the temperature sensors and amplifier inputs is a good practice to avoid long leads acting as antennas and picking up interference. However, the common-mode noise induced by the antenna can become normal mode at the point where the cables are connected to the circuit. This happens because of the difference between the terminal impedance of the cable and the terminal impedance of receiver circuit [79]. In this case, a mitigation of the attack consists in adding terminating resistors to the contact points. EMI enclosures can also be used to block interference. However, openings in the shield are often required to accommodate switches, connectors, indicators, or to provide ventilation. These openings may compromise shielding effectiveness by providing paths for high-frequency interference to enter the circuit board [63]. Moreover, it requires a careful thermal modeling of the system [58]. Another approach consists of sensor shielding when the temperature sensor needs to be externally exposed. In this case, shielding is only effective against interference if it provides a low impedance path to ground. However, some data acquisition systems require the temperature sensor to be grounded, such as thermocouple or RTD probes used in industrial processes [69]. When both the shield and temperature sensors are grounded, a ground-loop current can appear to the amplifier input terminals due to the difference of potential developed between the sensor ground and the amplifier ground connection [31]. When the EMI induces common mode noise, the interference can pass through the ground of the shield, creating a ground-loop current that can potentially generate the rectification effect. Some techniques can reduce but not eliminate the phenomenon, such as making the shield connection to ground as close as possible to the sensor connection to ground, or using only the ground terminal of the amplifier to connect to the shield without connecting the shield to the amplifier end.

Active and Passive Filters. In the case of op-amps and in-amps, manufacturers apply low-pass filters at the amplifier input pins to reduce the EMI signal energy from the input lines. In IC temperature sensors that use an inverting op-amp (e.g., LM35), a filter capacitor is placed between equal value resistors, while in IC temperature sensors (e.g., LM335) that use non-inverting op-amp, the filter capacitor is directly connected to the op-amp input. Precision in-amps in RTD and thermocouples sensors use two low-pass filters to suppress common-mode signals in each input lane and one capacitor to suppress differential-mode signals between the two amplifiers input terminals [3]. These filters are not sufficient for a complete attack mitigation due to the lines asymmetry and frequency range with respect to our injected interference. For example, in thermocouples, the asymmetry between the lines is exacerbated due to the two different conductors tied together. For these reasons, high precision temperature instruments contain additional isolation circuits and active low-pass filters connected to the amplifier input terminals to isolate the field-side and system-side circuitry [15].

Another protection method uses a composition of instrumentation amplifiers: three in-amps, two of these correlated to one another and connected in antiphase [54].

Choke-based filters can be also used as alternative for in-amp input filtering [54]. Despite the good noise suppression, the materials used for the inductance cores can heavily affect the filter performance for high frequency EMI, making the system vulnerable to injection attacks [81].

Amplifier outputs also need to be protected from EMI, since the interference injected on an output line couples back into the amplifier input where they are rectified and appear again on the output as a DC offset. An RC filter and/or a ferrite bead in series with the amplifier output are the simplest and inexpensive solutions to reduce the DC offset. However, for temperature systems, the output filtering is often limited to the line frequency and its harmonics (50 Hz/60 Hz) due to the interference noise generated when systems operate from the main power supply [36, 60].

6.2 Software Defenses

Many current temperature control systems use multiple sensors to continuously monitor the thermal state of different measurement points, or as multiple temperature reference values [3, 42]. In critical infrastructure sectors such as energy and healthcare, redundant sensors are used to generate time-dependent estimates of the critical points [47, 68]. Similar to sensor redundancy, sensor fusion techniques might be used to combine data from different sensors in order to produce the best estimation of the true state of a system and decrease the system's dependence on a single sensor [46]. In systems that rely on temperature sensors, literature provides various software countermeasures based on sensor fusion [55, 57]. However, in our experiments we demonstrate how physical proximity causes similar temperature sensors to be affected by similar attack effects (see Fig. 13). In turn, this increases the difficulty for a sensor fusion algorithm to detect the anomalies in small and self-contained systems, such as thermal chambers, or incubators. In addition, complex sensor fusion techniques require building models of the attacks effects on different sensors, using machine learning-based or statistical techniques to recognize the anomalies [53]. Therefore, to cover all the possible attack effects, these approaches require accurate parameter tuning and an exhaustive training phase. This might not be feasible to achieve. Furthermore, if the attack gradually changes the sensor data, or the operating conditions of the system change overtime, the sensor fusion algorithms might not be able to recognize the attack from the normal system behavior.

Other techniques focus on detecting injection attacks at the process level. A process-level intrusion detection system monitors sensors to determine if the physical process drifts from the normal or expected behavior. Common approaches include building Linear Dynamical State-Space (LDS) models of the physical process, or use machine learning and data mining to detect anomalies in the system behavior [29]. Although such approaches might detect anomalous events, models are difficult to build, as they require high effort in simulating and testing all possible attack vectors, and building a complete and highly detailed model of the physical process and interaction is not always feasible. Furthermore, machine learning methods that do not require a model of the physical process involve critical feature extraction and parameter-tuning phases that are often hard to automate and update on the discovery of a new attack vector. In addition, the systems that implement these kind of techniques need to continuously check if each sensor measurement drifts from the normal behavior captured during the training phase, drastically augmenting the computational and power resource costs.

Sensor redundancy, process-based techniques, and sensor fusion may significantly increase the effort an adversary must make to conduct an attack. However, implementing sophisticated software-based defenses remains arduous in large-scale consumer electronic devices.

6.3 Hardware Anomaly Detection System

For critical applications where it is not possible to implement complete shielding, or an effective mitigation filtering of the system and the sensor(s) - such as incubators - detecting the presence of attack attempts becomes crucial for verifying and maintaining temperature data reliability. A detection circuit can be used as a trigger for emergency measures - such as activating a safe mode where the system restricts its reliance on sensor data. To defend against EMI on cardiac implantable medical devices, Foo Kune et al. [56] proposed a cardiac probe to cross-check whether readings from a cardiac signal coincides with the expected values. Wang et al. [80] proposed an additional microphone to detect resonating sound that can affect MEMS gyroscopes. Based on our results, an effective defense for temperature-sensor-based systems that maintains the reliability of the temperature data should account for the frequencies that can induce a rectification effect in the amplifier output signal. Based on this frequency analysis, manufacturers can modify the design of their system to detect and react to attacks in the frequency bands of EMI signals. We propose a hardware anomaly detector to identify malicious signal and provide feedback about the reliability of the measurement data.

Design of the Anomaly Detector. The EMI signal induced by our attack can appear in many different points close to the amplifier where isolation circuitry and filters don't properly block the high frequency signals. A detector that can measure these signals can be implemented by connecting a low noise amplifier (LNA) and a band-pass filter to the points (such as a trace or wire) sensitive to the malicious signal (Fig. 15). By adopting the superheterodyne technique typical of AM receivers [74], the EMI frequency bands that cause significant DC offset variations can be down-converted to an intermediate frequency (IF). Down-conversion can be achieved by using a mixer and local oscillator. As a result, the use of this technique allows for a "tunable filter", which we can utilize for a tunable detector. Once the signal is digitally converted, amplitude and phase information of the malicious signals at the intermediate frequency can be then analyzed by the processor: (1) providing feedback on the temperature data reliability, (2) allowing the estimation of the measurement error, and (3) compensating it at the software level. The detector can be periodically activated when a temperature measurement is required. A variable oscillator can be used to select multiple vulnerable frequency bands.

Simulation Model and Evaluation. We simulate the detector against attacks on thermocouple sensors of the same type used in

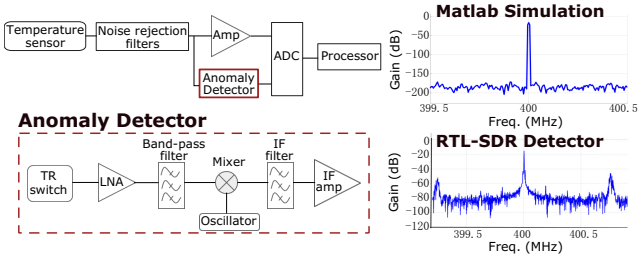

Figure 15: Block diagram and calculated gain of the anomaly detector based on superheterodyne method.

the thermal chamber. In this simulation, our detector can detect signals from 550 MHz to 1 GHz - the range which major affected the sensor (shown in Fig. 6). The simulation was designed using the Simulink environment [16], and consists of an LNA filter with 50 dB gain 3-order Butterworth band-pass filter, followed by a mixer block to down-convert the simulated EMI frequency to an IF frequency of 400 MHz, and an IR filter for filtering the spectral image components. Then, a subsequent 3-order Butterworth IF filter block is followed by an IF amplifier block with 100 dB gain and a noise figure of 2.5 dB. An RF Blockset testbench is used to simulate the EMI injection attack with an emitting power of 35 dBm.

To evaluate our design, we use a Software-Defined Radio (SDR) RTL-SDR device [61]. We choose the Realtek RTL2832U chipset with the R820T2 tuner chip that can detect frequencies from 500 kHz up to 1.75 GHz. An RF exposed connection, collocated with the temperature sensor breakout board, is followed by an RF filter and an LNA amplifier at 50 dB. A mixer with a local oscillator is used for the frequency transposition. The detector also uses Automatic Gain Control (AGC), where the gain varies with the available input power level. As a proof of concept demonstration, we successfully selectively detect a malicious signal at a 3 meter distance from the transmitting antenna, in open air, at a frequency of 503 MHz (corresponding to one of the major effective peaks in Fig. 6). The signal is down-converted to 400 MHz (as shown in Fig. 15). By varying the local oscillators frequency, the detector can also isolate the other vulnerable frequency bands.

7 RELATED WORK

Analog sensor circuits are especially susceptible to EMI. Various works demonstrate the exploitability of the non-linearities of different circuit components to cause system malfunctions or sensor misreadings (see Table 2).

Foo Kune et al. [56] showed that bogus signals can be injected through low-power EMI into analog sensors such as microphones, and implantable medical devices such as pacemakers and defibrillators. Their attack method exploited the generation of sub-harmonics of injected high frequency signals passing through common circuit components (e.g. wires, capacitors, amplifiers, and ADCs). This unintentional demodulation effect down-converts the high frequency signals into low frequency ones. In turn, these low frequency signals are able to pass the protective low-pass filters and enter into the system, compromising its functionality. In automotive field, Yan et al. [85] intentionally saturated Millimeter-Wave Radar by injecting strong interference, causing sensor denial-of-service in cars. Unlike these previous works, our EMI injection exploits the rectification effect present in the internal circuitry of operational and instrumentation amplifiers used in temperature-based control systems.

Delsing et al. [35] and Esteves et al. [37] empirically observed the general reaction of specific cyber-physical systems under strong interference. Delsing et al. verified the susceptibility of a MULLE node sensor network [48]. They observed disturbances in the Bluetooth communication, data losses and occasionally rebooting of the sensor network node. They also tested the sensor interface using a temperature sensor, revealing a vulnerability of the device due to the use of a long non-shielded connection between the sensor and the MULLE-device. Esteves et al. investigated a common-off-the-shelf (COTS) civilian quadricopter. They listed several reading errors induced in the drone sensors and interfaces by continuous interference, without exploring the causality of the measured effect.

Recent studies [33, 70, 71] investigated the injection of strong near-field interference to modify the input voltage of GPIO pins in microcontrollers. In particular, the authors used EMI injection to induce a rectification effect in the Electr-Static Discharge (ESD) protection circuit. The ESD protection circuit is used in microcontrollers GPIO pins to prevent the ADCs to be exposed to out-of-band input voltage when connected to an external analog or a digital sensor. In contrast with these works, our rectification attack directly affects the sensor amplification stage, and in particular the internal transistors in analog sensor amplifiers, before the connection with a microcontroller or the analog-to-digital conversion stage. In addition, instrumentation and operational amplifiers that work with low bias currents such as in temperature sensors, often do not implement external ESD protection circuits at the amplifier input, but only external current limiting resistors [32]. This approach is used because it provides adequate protection against overvoltage, it does not provoke high current leakage at increasing temperature as it happens using ordinary diodes, and the resistors are already present in the signal conditioning chain, since they constitute part of the low-pass filters used to reject differential and common-mode noise.

Physical-level Attacks on Sensors. Sensors are fundamental for cyber-physical systems such as autonomous vehicles, drones, and medical devices. Existing security studies on sensors have shown how they can be compromised by different kinds of signal injections other than EMI such as mechanical waves (i.e. sound), and light. For instance, by injecting different types of light signal using lasers, Park et al. [64] compromised medical infusion pumps to make them over/under-infuse, while Petit et al. [66] and Shin et al. [72] generate fake obstacles in LiDARs systems for automotive applications. Other works demonstrate how intense acoustic waves can incapacitate or manipulate some models of micro-electro-mechanical systems (MEMS) inertial sensors [73, 76, 77, 80], while Zhang et al. [86] used ultrasonic waves to send inaudible commands to voice assistance systems, such as Google Home and Alexa. Similar to our work, these attacks modulate the malicious signal on top of a carrier to infiltrate the system. However, they exploit different physical phenomena, such as the demodulation effect, or aliasing, rather than rectification. For this reason, defenses that mitigate these effects might be not sufficient to mitigate rectification attacks, since the physics principle exploited is different.

Table 2: Comparisons between previous studies and our work, including the targeted systems, the affected components, and the effect induced by the attacks.

Paper	System	Exploited Non-linearity Effect				Affected Component					
		Demodulation	Saturation	Aliasing	Rectification	Transd.	Wire	Filter	Amp.	ADC	GPIO
[56]	Microphone	●	○	●	○	●	●	●	●	●	○
	Implantable Medical Dev.	○	◐	○	○	○	●	●	○	○	○
[85]	Radar	○	●	○	○	●	○	○	●	○	○
[33, 70, 71]	Microcontroller	○	○	○	●	○	○	○	○	●	●
[35]	Sensor Network	○	◐	◐	◐	○	●	◐	◐	◐	◐
[37]	Drone	○	◐	◐	○	◐	◐	◐	◐	◐	○
Our work	Temperature Sensor	○	○	○	●	○	○	●	●	○	○

●Verified ◐Uncertain/Unverified ○Not applicable

The novelty of our work stands on this new attack vector not yet explored by previous research on sensor attacks. Further, we show how this vulnerability of amplifiers can affect different analog temperature sensors that use similar signal conditioning process.

8 DISCUSSIONS

8.1 Limitations

In our study we only consider commercial temperature-based systems that use analog temperature sensors. Our analysis focuses on low-power attacks (less than 4 W) in the Ultra High Frequency range (UHF) 300 MHz - 3 GHz. These assumptions are acceptable considering that our work shows how the rectification attack can be successful with a low-power injection, even if the target system already employs traditional EMI defenses. Also, we assume that an adversary can attempt the attack with little effort by building a small device or modifying a commercial system (e.g. a walkie-talkie) that can emit EMI signals in the vulnerable frequency range. Although the attack distance can be increased with specialized equipment and higher transmitting power, our goal is to demonstrate that simple amplitude-modulated EMI can induce a controllable voltage offset in temperature sensing circuits large enough to deceive and manipulate a target system.

To improve the attack success rate, an adversary might need some additional information regarding the target device, such as the presence of automatic temperature alarms and their threshold values. These information can be retrieved from the publicly available manuals and datasheets of the target system.

During our experiments, we observe that the amount of induced DC offset can be affected by various factors, including the noise rejection circuitry and shield used in the target system, the characteristics of the antenna used to perform the attack (e.g., directional, monopole, etc.) and its orientation with respect to the target device. In addition, to optimize the attack effect, the adversary often needs to position the antenna to target the parts of the victim system that are usually more susceptible (e.g., the temperature sensor transducer, the control panel, etc.).

8.2 Attack Generalization

By exploiting this hardware-level vulnerability, adversaries could also affect systems equipped with different classes of sensors that use similar signal conditioning processes. For example, we find that pressure or pH sensors may also be susceptible to adversarial control through rectification attacks, since the transducer signal of these sensors is weak and requires an amplification stage similar to temperature sensors.

Pressure Sensor. Scales use pressure sensors to measure the weight of an object. Sensor wires distributed inside of the device can make it vulnerable to EMI injection. We test a CGOLDENWALL high-precision lab digital scale that has an accuracy of 0.01 g, which can be used in jewelry, laboratory measurements. We are able to decrease the reading of the scale by 6.37 g at a distance of 0.5 m with an attack frequency of 685 MHz. We also test an Escali L600 L-Series High Precision Lab Scale. At an attack distance of 0.5 m, we can decrease the reading of the scale by 7 g, or increase the reading by 13.9 g. Using the same attack technique we show in this work, adversaries might be able to spoof the pressure or force measurement in data acquisition or control systems to cause unexpected consequences.

PH Sensor. A pH meter measures a low-level difference in electrical potential between a pH electrode and a reference electrode. We test an Apera Instruments PH700 Benchtop Lab pH Meter that has an accuracy of 0.01 pH. At an attack distance of 0.5 m, we can increase the measured pH value by 0.42 with EMI signal injections at a frequency of 515 MHz. PH sensors can be used in closed-loop control in SCADA systems such as water treatment facilities. Adversaries might attempt to manipulate the actual pH value to damage the facilities of such systems by exploiting pH sensors.

9 CONCLUSION

Temperature-based control systems fundamentally rely on sensors to make critical decisions. So it is important to assess and improve the resilience of the system in situations when temperature sensors could be compromised. This work showed how adversaries can manipulate these systems to cause unexpected consequences, without tampering with the victim system or triggering temperature alarms. The attack leveraged an unintended rectification effect in amplifiers to control the DC voltage of temperature sensor signals. We validated the attack on sensors and investigated the threat on several real-world temperature control systems. Our experimental results showed that these systems blindly trust spoofed temperature sensor readings, leading to manipulated decision makings of a victim system. To mitigate the risks, we discussed several conventional defensive techniques, and proposed a prototype design of

an analog anomaly detector to ensure the integrity of temperature sensor signals.

Acknowledgments. We are in the process to coordinate with ICS-CERT to notify manufacturer companies whose sensors and devices we tested. This work is supported in part by US NSF under grants CNS-1812553 and CNS-1330142.

REFERENCES

[1] 1997. World Health Organization, Maternal and Newborn Health/Safe Motherhood. Thermal protection of the newborn: a practical guide. https://apps.who.int/iris/bitstream/handle/10665/63986/WHO_RHT_MSM_97.2.pdf.

[2] 2001. Franks Hospital. Babytherm 8000 WB Warming bed. Instructions for Use. Page: 18. http://www.frankshospitalworkshop.com/equipment/documents/infant_incubators/user_manuals/GinevriOGBPolyCare3Incubator-Usermanual.pdf.

[3] 2009. Analog Devices. RFI Rectification Concepts. https://www.analog.com/media/en/training-seminars/tutorials/MT-096.pdf.

[4] 2009. Revolutionary Science. Product descriptions of the RS-IF-202 Incufridge. https://wikisites.mcgill.ca/djgroup/images/4/41/Incufridge_19L_Model_RS-IF-202.pdf.

[5] 2011. Sun Electronic Systems. Model EC1X environmental chamber user and repair manual. http://eecs.oregonstate.edu/matdev/man/Sun_Electronic_Systems_Environmental_Chamber_EC1X.PDF.

[6] 2011. World Health Organisation (WHO). Core Medical Equipment: Incubator, Infant (Page 31). http://apps.who.int/medicinedocs/documents/s22062en/s22062en.pdf.

[7] 2011. World Health Organisation (WHO). The blood cold chain. https://www.who.int/bloodsafety/processing/who_eht_11_04_en.pdf.

[8] 2013. Champlain Maternal Newborn Regional Program (CMNRP). Newborn Thermoregulation Self-Learning Module. http://www.cmnrp.ca/uploads/documents/Newborn_Thermoregulation_SLM_2013_06.pdf.

[9] 2015. Sparkfun. Schematics of the SparkFun MAX31855K Thermocouple Breakout. https://cdn.sparkfun.com/datasheets/Sensors/Temp/SparkFun_Thermocouple_Breakout_v10.pdf.

[10] 2015. World Health Organisation (WHO). Vaccine management handbook: How to monitor temperatures in the vaccine supply chain. https://apps.who.int/iris/bitstream/handle/10665/183583/WHO_IVB_15.04_eng.pdf.

[11] 2018. Adafruit. Analog Output K-Type Thermocouple Amplifier - AD8495 Breakout. https://www.adafruit.com/product/1778.

[12] 2018. Centers for Disease Control and Prevention (CDC). Vaccine Storage and Handling. https://www.cdc.gov/vaccines/pubs/pinkbook/vac-storage.html.

[13] 2018. Franks Hospital. Air Shields Isolette C-100, C-200 Infant Incubator Service manual. Section:7. http://www.frankshospitalworkshop.com/equipment/documents/infant_incubators/service_manuals/Air-Shields_Isolette_C-100,C-200_Infant_Incubator_-_Service_manual.pdf.

[14] 2018. International Biomedical. AirBorne 185A+ Transport Incubator Service Manual. https://www.int-bio.com/wp-content/uploads/2016/06/185A-Service-Manual-English-Rev-C.pdf.

[15] 2018. IOtech. Grounding and Shielding Considerations for Thermocouples, Strain Gages, and Low-Level Circuits. http://www.mccdaq.com/pdfs/techtip/techtip_60201.pdf.

[16] 2018. Mathworks. Superheterodyne Receiver Using RF Budget Analyzer App. https://www.mathworks.com/help/rf/examples/superheterodyne-receiver-using-rf-budget-analyzer-app.html.

[17] 2018. Minicircuits ZHL-4240W broad-band amplifier. https://www.minicircuits.com/pdfs/ZHL-4240W.pdf.

[18] 2018. Omega Co. Introduction to Resistance Temperature Detectors. https://www.omega.com/prodinfo/rtd.html.

[19] 2018. RFSpace LPDAMAX Wide-band PCB Log Periodic Antenna . http://rfspace.com/RFSPACE/Antennas_files/LPDA-MAX.pdf.

[20] 2018. Southwest Heater & Controls. Limit and Alarm Controllers. https://www.swhc.com/limit-alarm-controller.htm.

[21] 2018. Temperature Controller Basics Handbook. https://www.instrumart.com/pages/283/temperature-controller-basics-handbook.

[22] 2018. West Control Solutions Co. Temperature Monitors and Limiters. https://www.west-cs.com/assets/Brochures/BR-LD-2-US-1903-web-1.0.pdf.

[23] 2019. Adafruit. Digital Output PT100 RTD Temperature Sensor Amplifier - MAX31865 Breakout. https://www.adafruit.com/product/3328.

[24] 2019. Centers for Disease Control and Prevention (CDC). Vaccine Storage and Handling Toolkit. https://www.cdc.gov/vaccines/hcp/admin/storage/toolkit/storage-handling-toolkit.pdf.

[25] 2019. Great Ormond Street Hospital for Children - Clinical Guidelines: Thermoregulation for neonates. https://www.gosh.nhs.uk/health-professionals/clinical-guidelines/thermoregulation-neonates.

[26] 2019. Thermal Chamber Applications . https://www.intestthermal.com/products/chambers/applications.

[27] 2019. World Health Organisation (WHO). Blood cold chain. https://www.who.int/bloodsafety/processing/cold_chain/en/.

[28] Roberto Antonucci, Annalisa Porcella, and Vassilios Fanos. 2009. The infant incubator in the neonatal intensive care unit: unresolved issues and future developments. *Journal of perinatal medicine* 37, 6 (2009), 587–598.

[29] Wissam Aoudi, Mikel Iturbe, and Magnus Almgren. 2018. Truth will out: Departure-based process-level detection of stealthy attacks on control systems. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*. ACM, 817–831.

[30] Edward F Bell. 2006. Servocontrol: Incubator and radiant warmer. *Iowa Neonatology Handbook* (2006).

[31] Robert P Benedict and RJ Russo. 1972. A note on grounded thermocouple circuits. *Journal of Basic Engineering* 94, 2 (1972), 377–380.

[32] James Bryant. 2000. Protecting Instrumentation Amplifiers-All data acquisition board designs have to contend with ESO, EMI, and overvoltages. Can one solution protect the circuitry against all three hazards? *Sensors-the Journal of Applied Sensing Technology* 17, 4 (2000), 62–69.

[33] A. Ware David. 2017. *Effects of Intentional Electromagnetic Interference on Analog to Digital Converter Measurements of Sensor Outputs and General Purpose Input Output Pins.* Ph.D. Dissertation. Utah State University.

[34] Pauline Décima, Erwan Stéphan-Blanchard, André Léké, Loic Dégrugilliers, Stéphane Delanaud, Jean-Pierre Libert, and Pierre Tourneux. 2013. Does the incubator control mode influence outcomes of low-birth-weight neonates during the first days of life and at hospital discharge? *Health* 5, 08 (2013), 6.

[35] Jerker Delsing, Jonas Ekman, Jonny Johansson, Sofia Sundberg, Mats Bäckström, and T Nilsson. 2006. Susceptibility of sensor networks to intentional electromagnetic interference. In *International Zürich Symposium on Electromagnetic Compatibility*.

[36] Matthew Lawrence Duff and Joseph Towey. 2010. Two Ways to Measure Temperature Using Thermocouples Feature Simplicity, Accuracy, and Flexibility. *A forum for the exchange of circuits, systems, and software for real-world signal processing* (2010).

[37] José Lopes Esteves, Emmanuel Cottais, and Chaouki Kasmi. 2018. Unlocking the Access to the Effects Induced by IEMI on a Civilian UAV. In *2018 International Symposium on Electromagnetic Compatibility (EMC EUROPE)*. IEEE, 48–52.

[38] Brian Evans. 2012. *Practical 3D printers: The science and art of 3D printing*. Apress.

[39] Antonio Feteira. 2009. Negative temperature coefficient resistance (NTCR) ceramic thermistors: an industrial perspective. *Journal of the American Ceramic Society* 92, 5 (2009), 967–983.

[40] Franco Fiori. 2015. An analog front end based on chopped signals highly immune to RFI. In *Electromagnetic Compatibility (APEMC), 2015 Asia-Pacific Symposium on*. IEEE, 98–101.

[41] F. Fiori. 2016. A Sensor Signal Amplifier Resilient to EMI. *IEEE Sensors Journal* 16, 18 (2016), 7008–7015.

[42] Jeff Frolik, Mohamed Abdelrahman, and Param Kandasamy. 2001. A confidence-based approach to the self-validation, fusion and reconstruction of quasi-redundant sensor data. *IEEE Transactions on Instrumentation and Measurement* 50, 6 (2001), 1761–1769.

[43] Jerry Gaboian. 2000. A statistical survey of common-mode noise. *Analog Applications* (2000).

[44] Sandra Lee Gardner, Brian S Carter, Mary I Enzman-Hines, and Jacinto A Hernandez. 2011. *handbook of neonatal intensive care.* St Louis: Mosby Elsevier. 117–123 pages.

[45] Julie A Gazmararian, Natalia V Oster, Diane C Green, Linda Schuessler, Kelly Howell, Janona Davis, Marybeth Krovisky, and Samuel W Warburton. 2002. Vaccine storage practices in primary care physician offices: assessment and intervention. *American journal of preventive medicine* 23, 4 (2002), 246–253.

[46] Radoslav Ivanov, Miroslav Pajic, and Insup Lee. 2016. Attack-Resilient Sensor Fusion for Safety-Critical Cyber-Physical Systems. *ACM Trans. Embedded Comput. Syst.* 15 (2016), 21:1–21:24.

[47] Xin Jin, Asok Ray, and Robert M Edwards. 2009. Redundant Sensor Calibration and Estimation for Monitoring and Control of Nuclear Power Plants. *Transactions of the American Nuclear Society* 101 (2009), 307–308.

[48] Jonny Johansson, Matthias Völker, Jens Eliasson, Åke Östmark, Per Lindgren, and Jerker Delsing. 2004. Mulle: a minimal sensor networking device: implementation and manufacturing challenges. In *IMAPS Nordic Annual Conference: 26/09/2004-28/09/2004*. International Microelectronics and Packaging Society, Nordic chapter, 265–271.

[49] Ericalyn Kasdorf and Jeffrey M Perlman. 2013. Hyperthermia, inflammation, and perinatal brain injury. *Pediatric Neurology* 49, 1 (2013), 8–14.

[50] Chaouki Kasmi and José Esteves. 2018. Remote and Silent Voice Command Injection on a Smartphone through Conducted IEMI - Threats of Smart IEMI for Information Security. Wireless Security Lab, French Network and Information Security Agency (ANSSI), Tech. Rep. System Design & Assessment Note 48. http://ece-research.unm.edu/summa/notes/SDAN/SDAN0048.pdf. (04 2018).

[51] Walt Kester. 1999. *Practical design techniques for sensor signal conditioning.* Analog devices.

[52] Walt Kester, James Bryant, and Walt Jung. 1999. Temperature sensors (Section 7). (1999).

[53] Bahador Khaleghi, Alaa Khamis, Fakhreddine O Karray, and Saiedeh N Razavi. 2013. Multisensor data fusion: A review of the state-of-the-art. *Information fusion* 14, 1 (2013), 28–44.

[54] Charles Kitchin and Lew Counts. 2004. *A designer's guide to instrumentation amplifiers.* Analog Devices.

[55] Fan-Tian Kong, You-Ping Chen, Jing-Ming Xie, and Zu-De Zhou. 2005. Distributed temperature control system based on multi-sensor data fusion. In *Machine Learning and Cybernetics, 2005. Proceedings of 2005 International Conference on*, Vol. 1. IEEE, 494–498.

[56] Denis Foo Kune, John Backes, Shane S Clark, Daniel Kramer, Matthew Reynolds, Kevin Fu, Yongdae Kim, and Wenyuan Xu. 2013. Ghost talk: Mitigating EMI signal injection attacks against analog sensors. In *IEEE Symposium on Security and Privacy.*

[57] Santhosh KV and Karel De Smet. 2016. Sensor Data Fusion Framework for Improvement of Temperature Sensor Characteristics. *Measurement and Control* 49, 7 (2016), 219–229.

[58] Jaeho Lee, David W Gerlach, and Yogendra K Joshi. 2008. Parametric thermal modeling of heat transfer in handheld electronic devices. In *Thermal and Thermomechanical Phenomena in Electronic Systems, 2008. ITHERM 2008. 11th Intersociety Conference on.* IEEE, 604–609.

[59] Martha J Mance. 2008. Keeping infants warm: challenges of hypothermia. *Advances in neonatal care* 8, 1 (2008), 6–12.

[60] McCarthy Mary and Dillon Eamonn. 2006. ADC Requirements for Temperature Measurement Systems. https://www.analog.com/media/en/technical-documentation/application-notes/AN-880.pdf?doc=UG-181.pdf.

[61] M. Mishra, A. Potnis, P. Dwivedy, and S. K. Meena. 2017. Software defined radio based receivers using RTL-SDR: A review. In *2017 International Conference on Recent Innovations in Signal processing and Embedded Systems (RISE).*

[62] Y Molgat-Seon, T Daboval, S Chou, and O Jay. 2013. Accidental overheating of a newborn under an infant radiant warmer: a lesson for future use. *Journal of Perinatology* 33, 9 (2013), 738.

[63] Ralph Morrison. 1977. *Grounding and shielding techniques in instrumentation.* Wiley New York.

[64] Youngseok Park, Yunmok Son, Hocheol Shin, Dohyun Kim, and Yongdae Kim. 2016. This Ain't Your Dose: Sensor Spoofing Attack on Medical Infusion Pump. In *10th USENIX Workshop on Offensive Technologies (WOOT).*

[65] Elizabeth Payne. 2016. A Brief History of Advances in Neonatal Care. https://www.nicuawareness.org/blog/a-brief-history-of-advances-in-neonatal-care.

[66] Jonathan Petit, Bas Stottelaar, and Michael Feiri. 2015. Remote Attacks on Automated Vehicles Sensors : Experiments on Camera and LiDAR.

[67] AS Poulton. 1994. Effect of conducted EMI on the DC performance of operational amplifiers. *Electronics letters* 30, 4 (1994), 282–284.

[68] Asok Ray and Rogelio Luck. 1991. An introduction to sensor signal validation in redundant measurement systems. *IEEE Control Systems* 11, 2 (1991), 44–49.

[69] David Ross-Pinnock and Paul G Maropoulos. 2016. Review of industrial temperature measurement technologies and research priorities for the thermal characterization of the factories of the future. In *Proceedings of the Institution of Mechanical Engineers, Part B: Journal of Engineering Manufacture*, Vol. 230. 793–806.

[70] Jayaprakash Selvaraj. 2018. *Intentional Electromagnetic Interference Attack on Sensors and Actuators.* Ph.D. Dissertation. Iowa State University.

[71] Jayaprakash Selvaraj, Gökçen Y Dayanıklı, Neelam Prabhu Gaunkar, David Ware, Ryan M Gerdes, Mani Mina, et al. 2018. Electromagnetic Induction Attacks Against Embedded Systems. In *Proceedings of the 2018 on Asia Conference on Computer and Communications Security.* 499–510.

[72] Hocheol Shin, Dohyun Kim, Yujin Kwon, and Yongdae Kim. 2017. Illusion and Dazzle: Adversarial Optical Channel Exploits against Lidars for Automotive Applications. In *International Conference on Cryptographic Hardware and Embedded Systems.* Springer.

[73] Yunmok Son, Hocheol Shin, Dongkwan Kim, Youngseok Park, Juhwan Noh, Kibum Choi, Jungwoo Choi, and Yongdae Kim. 2015. Rocking Drones with Intentional Sound Noise on Gyroscopic Sensors. In *Proceedings of USENIX Security Symposium.*

[74] C. Stagner, A. Conrad, C. Osterwise, D. G. Beetner, and S. Grant. 2011. A Practical Superheterodyne-Receiver Detector Using Stimulated Emissions. *IEEE Transactions on Instrumentation and Measurement* 60, 4 (2011), 1461–1468.

[75] Hugh Tilson, Marilyn J Field, et al. 2006. *Safe Medical Devices for Children. Chapter: 4 Identifying and Understanding Adverse Medical Device Events. (Page 147-148).* National Academies Press.

[76] Timothy Trippel, Ofir Weisse, Wenyuan Xu, Peter Honeyman, and Kevin Fu. 2017. WALNUT: Waging doubt on the integrity of MEMS accelerometers with acoustic injection attacks. In *Proceedings of IEEE European Symposium on Security and Privacy.*

[77] Yazhou Tu, Zhiqiang Lin, Insup Lee, and Xiali Hei. 2018. Injected and Delivered: Fabricating Implicit Control over Actuation Systems by Spoofing Inertial Sensors. In *Proceedings of USENIX Security Symposium.*

[78] Edward James Walter and Mike Carraretto. 2016. The neurological and cognitive consequences of hyperthermia. *Critical Care* 20, 1 (2016), 199.

[79] Shuo Wang and Fred C Lee. 2010. Analysis and applications of parasitic capacitance cancellation techniques for EMI suppression. *IEEE Transactions on Industrial Electronics* 57, 9 (2010), 3109–3117.

[80] Zhengbo Wang, Kang Wang, Bo Yang, Shangyuan Li, and Aimin Pan. 2017. Sonic gun to smart devices: Your devices lose control under ultrasound/sound. *BlackHat USA* (2017).

[81] S Weber, M Schinkel, E Hoene, S Guttowski, W John, and H Reichl. 2005. Radio frequency characteristics of high power common-mode chokes. In *IEEE Int. Zurich Symp. on Electromagnetic Compatibility.* 1–4.

[82] Melanie Welte. 2007. USA Today: Vaccines ruined by poor refrigeration. https://usatoday30.usatoday.com/news/health/2007-12-04-spoiled-vaccines_N.htm.

[83] David Weston. 2016. *Electromagnetic Compatibility: Methods, Analysis, Circuits, and Measurement.* Crc Press.

[84] Chunyu Wu, Guanghua Li, David J Pommerenke, Victor Khilkevich, and Gary Hess. 2018. Characterization of the RFI Rectification Behavior of Instrumentation Amplifiers. In *2018 IEEE Symposium on Electromagnetic Compatibility, Signal Integrity and Power Integrity (EMC, SI & PI).* IEEE, 156–160.

[85] Chen Yan, Wenyuan Xu, and Jianhao Liu. 2016. Can you trust autonomous vehicles: Contactless attacks against sensors of self-driving vehicle. *DEF CON* 24 (2016).

[86] Guoming Zhang, Chen Yan, Xiaoyu Ji, Tianchen Zhang, Taimin Zhang, and Wenyuan Xu. 2017. DolphinAttack: Inaudible voice commands. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security.*

APPENDIX

The Setup of DPI Experiments on the Experimental Temperature Sensing Circuitry

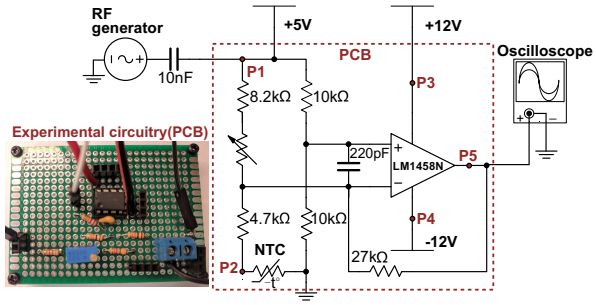

Figure 16: The setup of direct power injections through different injection points of a typical NTC-based temperature sensing circuitry. In this illustration, the signal injection circuit is connected to the injection point P1.

As shown in Fig. 16, a 1-meter NTC thermistor is wired in a bridge circuit, which is excited by a $+5V$ DC power source. The differential voltage generated by the bridge circuit is collected and amplified by a Texas Instruments (TI) LM1458 operational amplifier. By measuring the output voltage of the amplifier, the resistance of the thermistor and the corresponding temperature can be calculated. We choose the circuit elements based on the schematics of temperature sensing circuits in infant incubators [13, 14]. During the experiments, the $+5V$ and $\pm 12V$ DC voltage sources are provided by an Agilent E3630A triple output power supply. We monitor the analog amplified output with an Agilent MSOX4054A oscilloscope.

In our DPI experiments, we connect the output of the signal injection circuit to each of the signal injection points on the sensing circuitry. A $10nF$ capacitor is used to decouple the DC signal in the experimental circuitry from the signal injection circuitry. The source of the EMI signals is an Agilent N5172B vector signal generator.